DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

SEP 18 2002

IN REPLY
REFER TO: Chief Information Officer (CIO)

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Default Passwords

1. All operating systems arrive from the vendor or manufacturer with commonly known standard factory default passwords. Exploitation of these default accounts and passwords is the easiest way to gain unauthorized access to any system. In fact, the Systems Administration, Audit, Network Security (SANS) Organization cites "The Default Password Threat" as one of its "Ten Most Critical Internet Security Threats." In January 2002, the Computer Emergency Response Team (CERT) Coordination Center issued an alert (VU#712723) to raise awareness of this common vulnerability.

2. DISA Field Security Operations (FSO) has identified the default password vulnerability as the most prevalent high-risk vulnerability in the majority of the Security Readiness Reviews (SRRs) conducted in DISA over the last three years. This vulnerability is considered a Category I finding and represents a significant impediment to maintaining a secure operating environment. FSO noted an alarming and rising increase of this deficiency in environments using Oracle. It appears the number of default accounts and passwords in Oracle increases with every version and release. It should also be noted that information related to default accounts and passwords is widely available via the Internet. Consult the following sites for more information:

http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf, http://www.nextgenss.com/papers/hpoas.pdf, and http://www.pentest-limited.com/default-user.pdf.

3. The ability to define, configure, and maintain a secure operating environment is a fundamental system administrator responsibility. I am requesting that each system administrator review their list of systems and privileges for any default accounts and passwords to either delete or disable the account or change the password.

4. Finally, all DISA systems, networks, and databases are to be configured for security by consulting the appropriate Security Technical Implementation Guide (STIG). The DISA STIGs and their respective checklists and scripts are available at the DISA Information Assurance Support Environment (IASE) Web Server. The server URL is https://iase.disa.mil/.

5. Increasing attacks against the Department of Defense's information infrastructure have heightened awareness of the importance of protecting our information resources against modern day cyber attacks in a 'shared risk' environment. Our mission to protect and secure the DoD infrastructure dictates that we apply rigorous standards to increase our operational security effectiveness. Questions concerning this memorandum may be directed to Ms. Regina Meehan, CIO/IAD, DSN 761-4688, Comm (703) 681-4688 or email meehanr@ncr.disa.mil.

Shirley L. Fields

SHIRLEY L. FIELDS
Chief Information Officer

Distribution:
Director (D)
Vice Director (DV)
Command Chief Master Sergeant (D/SEA)
Chief of Staff (COS)
General Counsel (GC)
Inspector General (IG)
Small and Disadvantaged Business Utilization (SADBU)
Protocol
Equal Employment Opportunity & Cultural Diversity (EEO&CD)
Congressional Affairs (CR)
Chief Financial Executive/Comptroller (CFE/DC)
Chief Information Officer (CIO)
Chief Information Assurance Executive (CIAE)
Chief Technical Officer (CTO)
Chief Transformation Executive (CTE)
Principal Director for Applications Engineering (AP)
Principal Director for Computing Services (CSD)
Principal Director for Customer Advocacy (CA)
Principal Director for Interoperability (IN)
Principal Director for Network Services (NS)
Principal Director for Operations (OP)
Director for Acquisition, Logistics, and Facilities (AQ)
Director for Manpower, Personnel, and Security (MPS)

DISA Memo, CIO, Default Passwords

Director for Strategic Plans, Programming, and Policy (SP3)
Director for Technical Integration Services (TIS)
Deputy Manager, National Communications System (NC)
Commander, White House Communications Agency (WHCA)
Commander, White House Situation Support Staff (WHSSS)
Administrator, Defense Technical Information Center (DTIC)
Commander, Joint Interoperability Test Command (JITC)
Commander, Joint Staff Support Center (JSSC)
Commander, Joint Spectrum Center (JSC)
Commander, DISA CENTCOM/SOCOM
Commander, DISA EUR
Commander, DISA JFCOM
Commander, DISA PAC
Commander, DISA SOUTHCOM
Commander, DISA SPACECOM
Commander, DISA STRATCOM
Commander, DISA TRANSCOM
Commander, DISA CONUS
Commander, DISA - Fort Gordon